Das Address-Resolution-Protocol

Michael Dienert

12. April 2019

Inhaltsverzeichnis

1 Mit tcpdump und arping ARP erforschen

Folgendes Experiment ist durchzuführen (Hinweis: die angegebene IP-Adresse und das Ethernet-Interface sind ggfs. anzupassen):

- In einem Konsolenfenster folgenden Befehl ausführen:

  ```
  ip a
  ```

  Das Interface suchen, das mit dem Schulnetz verbunden ist. Die IP-Adressen im Schulnetz haben die Form 10.20.23.xx.

- zu Root wechseln:

  ```
  sudo su
  ```

- Nun folgenden Befehl ausführen:

  ```
  tcpdump -ntXXi <interfacename> arp | grep -A15 10.20.23.100
  ```

- In einem zweiten Konsolenfenster folgendes Kommando ausführen:

  ```
  arping 10.20.23.100
  ```

- Das arping-Kommando mit ctrl-c und anschliessend das tcpdump-Kommando mit ctrl-c abbrechen, sobald die ersten ARP-Pakete angezeigt werden. Durch das grep-Filter kann es etwas dauern, bis man etwas zu sehen bekommt. Einige Sekunden Geduld!

- Im Anzeigepuffer des Terminal-Fensters die gewünschten ARP-Request und -Reply Frames suchen und analysieren

2 Lösung

2.1 arp-request

```
ARP, Request who-has 192.168.2.103 tell 192.168.2.101, length 28
        0x0000:  ffff ffff ffff 001c b3c3 830f 0806 0001  ................
        0x0010:  0800 0604 0001 001c b3c3 830f c0a8 0265  ...............e
        0x0020:  0000 0000 0000 c0a8 0267                 .........g
```

ffff ffff ffff : 6 Bytes Broadcast MAC-Adresse

001c b3c3 83 0f : 6 Bytes MAC-Adresse des Senders

0806 : Ethertype des Frames, 0806 = ARP

0001 : Hardwareadresstyp

0800 : Protokolladresstyp

0604 : Länge der H/W-Adresse=6, Länge der logischen Adresse=4

0001 ; Wert=1 $\Rightarrow$ ARP-Request (Wert=2 wäre ARP-Reply)

001c b3c3 83 0f : MAC-Adresse des Senders im ARP-Paket

c0a8 0265 : IP-Adresse des Senders (192.168.2.101) im ARP-Paket

0000 0000 0000 : MAC-Adresse des Ziels im ARP-Paket (noch unbekannt)

c0a8 0267 : IP-Adresse des Ziels (192.168.2.103) im ARP-Paket

2.2 arp-reply

```
ARP, Reply 192.168.2.103 is-at 00:14:51:84:93:c9, length 28
        0x0000:  001c b3c3 830f 0014 5184 93c9 0806 0001  ........Q.......
        0x0010:  0800 0604 0002 0014 5184 93c9 c0a8 0267  ........Q......g
        0x0020:  001c b3c3 830f c0a8 0265                 .........e
```

001c b3c3 830f : 6 Bytes Ziel MAC-Adresse

0014 5184 93c9 : 6 Bytes MAC-Adresse des Senders

0806 : Ethertype des Frames, 0806 = ARP

0001 : Hardwareadresstyp

0800 : Protokolladresstyp

0604 : Länge der H/W-Adresse=6, Länge der logischen Adresse=4

0002 ; Wert=2 $\Rightarrow$ ARP-Reply

0014 5184 93c9 : MAC-Adresse des Senders im ARP-Paket

c0a8 0267 : IP-Adresse des Senders (192.168.2.103) im ARP-Paket

001c b3c3 830f : MAC-Adresse des Ziels im ARP-Paket

c0a8 0265 : IP-Adresse des Ziels (192.168.2.101) im ARP-Paket